**UNITED STATES DISTRICT COURT**
**FOR THE NORTHERN DISTRICT OF TEXAS**
**DALLAS DIVISION**

**TRACY OCHE,** individually and on behalf of all others similarly situated,

Plaintiff,

v.

**NATIONAL MATH AND SCIENCE INITIATIVE**,

Defendant.

Case No.: 3:22-cv-834

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

Plaintiff Tracy Oche (hereinafter "Plaintiff") brings this class action (the "Action") against Defendant National Math and Science Initiative (hereinafter "Defendant" or "NMSI"), upon personal knowledge as to itself and its own actions, and upon information and belief, including the investigation of counsel as follows:

## I. NATURE OF THE ACTION

1. This Action arises out of the recent cyberattack and data breach at NMSI that targeted the information of students who utilized NMSI for educational services (the "Data Breach").

2. The Data Breach resulted in unauthorized access to the sensitive data of consumers, most of whom are students, who used NMSI's services. Because of the Data Breach, nearly 200,000 Class members suffered ascertainable losses, including out-of-pocket expenses and the value of their time spent attempting to remedy or mitigate the effects of the attack, and the present and substantial risk of imminent harm caused by the compromise of their sensitive personal information, including their name, test scores, Social Security number, date of birth, and student identification information (hereinafter, "Personally Identifiable Information" or "PII").

3. To compound matters, NMSI's Data Breach occurred from September 23, 2021 through October 18, 2021, and NMSI did not ascertain what information was accessed until January 6, 2022.

4. NMSI then sat on this information for over a month—failing to disseminate data breach consumer notifications until February 2022. When a data set that is inclusive of the aforementioned PII is breached, every moment is precious to affected consumers who seek to ensure their data is not weaponized against them through identity theft. Sitting on this information allowed NMSI to dodge responsibility and inevitably worsened the Data Breach victims' chances of weathering the storm that NMSI created.

5. As a result of the Data Breach, Plaintiff and Class members have been harmed—they have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class members must now and forever closely monitor their financial accounts to guard against identity theft.

6. Plaintiff and Class members may also incur out-of-pocket costs, for example, having to purchase credit monitoring systems, credit freezes, or other protective measures to deter and detect identity theft. Plaintiff seeks to remedy those harms on behalf of herself and all similarly situated persons whose PII was accessed unlawfully during the Data Breach. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement for out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems and protocols, future annual audits, and adequate credit monitoring services funded by the Defendant.

7. As such, Plaintiff brings this Action against Defendant seeking redress for its unlawful conduct and negligence.

## II. JURISDICTION AND VENUE

8. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 Class members and because the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Moreover, at least one member of the Class, and Defendant are citizens of different states.

9. The Court has general personal jurisdiction over Defendant because, personally or through its agents, Defendant operated, conducted, engaged in, or carried on a business or business venture in Texas; had offices in Texas; and committed tortious acts in Texas. Defendant is organized under the laws of Texas and headquartered in Dallas, Texas.

10. Venue is proper in this district under 28 U.S.C. §§ 1391(a)(1), 1391(b)(1), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this district, Defendant conducts substantial business in this District, and Defendant is a resident of this District. Further, Defendant is headquartered and does business in and/or has offices for the transaction of its customary business in this District in the Dallas Division.

## III. PARTIES

11. Plaintiff Tracy Oche is a citizen of Richardson, Texas and was harmed by the Data Breach alleged herein.

12. Defendant NMSI is an educational organization responsible for providing educational services around the United States and maintains its principal place of business at 8350 North Central Expressway, Suite 2200, Dallas, Texas 75206 in Dallas County, Texas. Through its various programs—including the College Readiness Program, through which it "encourages excellence" among Advanced Placement students at more than 1,400 public high schools across

36 States and the District of Columbia[1]—Defendant provided services to Class members scattered across the United States.

## IV. FACTUAL ALLEGATIONS

### DEFENDANT'S BUSINESS

13. According to the Defendant, NMSI "work[s] with local, state and national partners to increase education opportunities and empower better outcomes for all students."[2] NMSI's work is specific to a curriculum that is STEM-centric, as NMSI "believe[s] STEM education is the greatest lever to accessing opportunity and is unmatched in unlocking student potential."[3]

14. NMSI operates four separate programs through which it acquired the PII of Class members, including high school students. Those programs include the Teacher Pathways Program; Laying the Foundation; and the AlignEd Program.

15. NMSI's flagship program is its College Readiness Program, a "year-round and holistic support for school systems, teachers, students and communities." In addition to providing teachers with guides and teaching materials for use in their Advanced Placement courses, as well as access to an online forum in which they can interact with peers from across the country, the program also provides AP students with "access to live and on-demand study supports" and study resources aligned to their AP class."[4] In order to avail themselves of these resources however, teachers and students must first entrust their PII to Defendant.

16. According to NMSI's Privacy Policy, "NMSI is committed to protecting your privacy and providing you with a safe online experience."[5] The Privacy Policy states:

---

[1] https://www.nms.org/Our-Programs/Teachers/AP-Courses/CRP.aspx (last accessed Apr. 5, 2022).
[2] https://www.nms.org/About-Us.aspx, (last accessed Apr. 5, 2022).
[3] *Id.*
[4] https://www.nms.org/Our-Programs/Teachers/AP-Courses/CRP.aspx (last accessed Apr. 5, 2022).
[5] https://www.nms.org/getmedia/13f23a1c-59de-4062-b87f-319495996fcb/Privacy-Policy.pdf.aspx, (last accessed Apr. 5, 2022).

> NMSI collects personally identifiable information, such as your e-mail address, name, home or work address and telephone number. If you register on the NMSI Website, NMSI may also collect information regarding your education history and background, information regarding your current job and prior work history, demographic information such as gender, age and ethnicity, and other information designed to help NMSI provide services and information to you and/or to help NMSI understand the demographics of the people using the NMSI Website. …NMSI will also collect credit card information including credit card number, expiration date and card security code.
>
> Information about your computer hardware and software is automatically collected by NMSI for the operation of the NMSI Website and service, to maintain quality of the NMSI Website and service, and to provide general statistics regarding use of the NMSI Website. This information can include: your IP address, browser type, domain names, access times and referring Web site addresses.

17. With respect to data breaches in particular, the NMSI Privacy Policy states:

> If NMSI knows or learns of a security breach by an unauthorized party with respect to the NMSI Website, or that any user data or personal information collected by NMSI was accessed or used for an unauthorized purpose, NMSI will comply with all applicable data breach laws and regulations, and will use reasonable efforts to notify you of such security breach without unreasonable delay so that you can take appropriate actions.

18. By obtaining, collecting, using and deriving benefits from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting said PII from unauthorized disclosure.

19. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII.

## THE DATA BREACH

20. "[A] data breach exposes confidential, sensitive, or protected information to an unauthorized person. The files in a data breach are viewed and/or shared without permission."[6]

[6] "*How Data Breaches Happen*," KASPERSKY, at https://www.kaspersky.com/resource-center/definitions/data-breach (last accessed Mar. 15, 2022).

21. From September 23, 2021 through October 18, 2021, NMSI experienced a security incident involving unauthorized access to its file servers (the "Data Breach").

22. Defendant NMSI launched an investigation and determined that an unauthorized individual obtained access to files on its storage servers.

23. Defendant admits that it was not able to ascertain what information was accessed in the Data Breach until January 6, 2022.

24. However, despite determining the PII that was misappropriated during the Data Breach (and, presumably, the individuals whose PII was stolen) on January 6, 2022, Defendant waited more than a month to notify the victims of the Data Breach—finally notifying them on or around February 7, 2022.

25. The Data Breach resulted in malevolent actors accessing the sensitive data of nearly 200,000 geographically dispersed individuals—many of whom were minors when Defendant collected their PII.

26. The sensitive PII stolen in the Data Breach included Plaintiff's and Class members' name, test scores, Social Security number, date of birth, and student identification information. The third parties who exfiltrated this highly sensitive PII were able to do so because the files accessed during the Data Breach were not encrypted.

27. Plaintiff and Class Members provided their PII to Defendant with the reasonable expectation and the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access. Defendant's data security obligations were particularly important given the substantial increase in data breaches preceding the date of the breach.

28. Therefore, the increase in such attacks, and the attendant risk of future attacks was widely known to the public and to anyone in the Defendant's industry, including the Defendant itself.

## SECURING PII AND PREVENTING BREACHES

29. NMSI could have prevented this Data Breach by properly encrypting or otherwise protecting their equipment and computer files containing PII.

30. In its notice letters, NMSI acknowledged the sensitive and confidential nature of the PII, that the misuse or inadvertent disclosure of PII can pose major privacy and financial risks to impacted individuals, and that under state law they may not disclose and must take reasonable steps to protect PII from improper release or disclosure.

## THE DATA BREACH WAS A FORESEEABLE RISK

31. It is well known that PII, including Social Security numbers, is an invaluable commodity and a frequent target of hackers.

32. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[7]

33. Of the 1,473 recorded data breaches, 108 occurred the banking/credit/financial industry and resulted in the exposure of more than 100 million sensitive records. In fact, of the approximately 165 million sensitive records that were exposed in data breaches that occurred in 2019, nearly two-thirds of those records were exposed in the 108 breaches in the banking/credit/financial sector.[8]

[7] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed December 10, 2021)
[8] *Id.*

34. Individuals place a high value not only on their PII, but also on the privacy of that data. For the individual, identity theft causes significant negative financial impact on victims as well as severe distress and other strong emotions and physical reactions.

35. Individuals are particularly concerned with protecting the privacy of their and social security numbers. Neal O'Farrell, a security and identity theft expert for Credit Sesame, calls a Social Security number "your secret sauce," that is "as good as your DNA to hackers."

36. There are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their social security numbers have been accessed, Plaintiff and Class members cannot obtain new numbers unless they become a victim of Social Security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems . . . and won't guarantee . . . a fresh start."

37. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), NMSI knew or should have known that its electronic records would be targeted by cybercriminals.

38. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, take appropriate measures to prepare for, and are able to thwart such an attack.

39. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgment of its duty to keep PII private and secure,

NMSI failed to take appropriate steps to protect the PII of Plaintiff and the proposed Class from being compromised during a data breach.

## NMSI OWED A DUTY TO PLAINTIFF AND CLASS MEMBERS TO PROPERLY SECURE THEIR PII

40. At all relevant times, NMSI owed a duty to Plaintiff and Class members to properly secure their PII, encrypt and maintain such information using industry standard methods, train its employees to protect sensitive information, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff and Class members, and to *promptly* notify Plaintiff and Class members when NMSI became aware that their PII may have been compromised.

41. NMSI's duty to use reasonable security measures arose as a result of the special relationship that existed between NMSI, on the one hand, and Plaintiff and the Class members, on the other hand. The special relationship arose because Plaintiff and the members of the Class entrusted NMSI with their PII when they transacted with NMSI.

42. NMSI had the resources necessary to prevent the Data Breach but neglected to invest in adequate security measures, despite its obligation to protect such information. Accordingly, NMSI breached duties it owed to Plaintiff and Class members.

43. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

44. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[9] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[10]

45. The ramifications of NMSI's failure to keep Plaintiff's and Class members PII secure are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and the attendant damages victims suffer as a result are likely to continue for years.

**THE VALUE OF PII**

46. The PII of consumers is of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200.[11] According to the Dark Web Price Index for 2021, payment card details for an account balance up

[9] 17 C.F.R. § 248.201 (2013).
[10] *Id*.
[11] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Apr. 5, 2022).

to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.[12]

47. Social Security numbers are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[13]

48. Furthermore, trying to change or cancel a stolen Social Security number is no easy task. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

---

[13] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed December 10, 2021).

49. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[14]

50. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[15]

51. PII can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[16]

52. Given the nature of NMSI's Data Breach, as well as the length of the time NMSI's systems were breached and its long and inexcusable delay in notifying Class members, it is foreseeable that the compromised PII has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiff's and Class members' PII can easily obtain Plaintiff's and Class members' tax returns or open fraudulent credit card accounts in Class members' names.

53. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data

---

[14] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed December 10, 2021).

[15] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed December 10, 2021).

[16] *See* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1.

breach, because credit card victims can cancel or close credit and debit card accounts.[17] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

54. The injuries to Plaintiff and Class Members were directly and proximately caused by NMSI's failure to implement or maintain adequate data security measures for its current and former customers.

**DEFENDANT FAILED TO COMPLY WITH FTC GUIDELINES**

55. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision- making.

56. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[18] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[19]

---

[17] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes, Mar 25, 2020, *available at*: https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last accessed December 10, 2021).

[18] Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Mar. 15, 2022).

[19] *Id.*

57. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

58. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

59. Defendant failed to properly implement basic data security practices.

60. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

61. Defendant was at all times fully aware of its obligation to protect the PII of its subjects. Defendant was also aware of the significant repercussions that would result from its failure to do so.

62. Several best practices have been identified that at a minimum should be implemented by companies like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti- malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

63. Other best cybersecurity practices that are standard in the Defendant's industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

64. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

65. The foregoing frameworks constitute existing and applicable industry standards applicable to Defendant and its industry. Defendant's failure to comply therewith opened the door to and caused the Data Breach.

**DEFENDANT'S BREACH**

66. Defendant breached its obligations to Plaintiff and Class members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches;

b. Failing to adequately protect PII;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to train its employees in the proper handling of data breaches, the protection of PII, and the maintenance of adequate email security practices;

e. Failing to comply with the FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; and,

f. Failing to adhere to industry standards for cybersecurity.

67. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class members' PII by allowing cyberthieves to access NMSI's IT systems, which contained unsecured and unencrypted PII, to the detriment of Plaintiff and the Class.

**HARM TO CONSUMERS**

68. PII is such a valuable commodity to identity thieves that once the information is compromised, criminals often trade the information on the "cyber black- market" for years.

69. There is a strong probability that entire batches of information stolen from Defendant both have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class members are at an increased risk of fraud and identity theft for many years into the future.

70. Thus, Plaintiff and Class members must vigilantly monitor their financial accounts, credit reports, and identities for many years to come.

71. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the

suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

72. As such, there may be a significant time lag between when harm occurs versus when it is discovered, in addition to the significant time gap that may occur between the data breach when PII was stolen, and when the stolen PII is used.

73. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class members, including Social Security numbers, driver's license numbers, and financial account information, and of the foreseeable consequences that would occur if Defendant's data security system and network was breached, including, specifically, the significant costs the Data Breach would (and did) impose on Plaintiff and Class members.

74. Defendant knew or should have known about these dangers and strengthened its data, IT, and email handling systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

**HARM TO PLAINTIFF**

75. Prior to the Data Breach, Ms. Oche provided her PII to NMSI in connection with Advanced Placement classes in which she previously was enrolled while attending high school.

76. In February of 2022, Plaintiff received the Notice of Data Breach Letter from NMSI, in which NMSI informed her that her full name and social security number were stolen by cyberthieves in the Data Breach. As a result of the Data Breach, NMSI directed Plaintiff to take certain steps to protect her PII and otherwise mitigate damages.

77. As a result of the Data Breach and the directives that she received in the Notice Letter, Plaintiff spends approximately several hours per week dealing with the consequences of

the Data Breach, including, for example, self-monitoring her bank and credit accounts, as well spending time to verify the legitimacy of the *Notice of Data Breach*, communicating with her bank, and exploring credit monitoring and identity theft insurance options. This time has been lost forever and cannot be recaptured.

78. Plaintiff is very careful about sharing her own PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

79. Plaintiff stores any and all documents containing PII in a secure location, and destroys any documents she receives in the mail that contain any PII or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

80. As a direct result of NMSI's conduct, including the mismanagement of her PII before and during the Data Breach, Plaintiff suffered actual injury and damages.

81. Plaintiff suffered actual injury in the form of damages and diminution in the value of her PII—a form of intangible property that she entrusted to NMSI for the purpose of providing her with educational services, which was compromised in and as a result of the Data Breach.

82. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and she has suffered anxiety and increased concerns for the theft of her privacy since she received the Notice Letter. She is especially concerned about the theft of her full name paired with her Social Security number.

83. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her stolen PII, especially her Social Security number, being placed in the hands of unauthorized third-parties and possibly criminals.

84. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in NMSI's possession, is protected and safeguarded from future breaches.

## V. CLASS ALLEGATIONS

85. Plaintiff brings this Action on behalf of herself and on behalf of all other persons similarly situated (the "Class"). Plaintiff proposes the following Class definition, subject to amendment as appropriate:

**All persons whose PII was accessed in the Data Breach.**

Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Also excluded from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

86. In the alternative, Plaintiff brings this action on behalf of herself and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a subclass of:

> All persons who are residents of the State of Texas whose PII was accessed in the Data Breach (the "Texas Subclass").

Excluded from the Texas Subclass are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant, as well as members of the judiciary to whom this case is assigned, their families and members of their staff.

87. **Numerosity**. The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class members is unknown to Plaintiff at this time, based on information and belief, the Class consists of over 191,000 individuals whose sensitive data was compromised in the Data Breach.

88. **Commonality**. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

A. Whether the Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class members' Personally Identifiable Information;

B. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

C. Whether Defendant's data security systems prior to, during, and after the Data Breach complied with the applicable data security laws and regulations;

D. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards, as applicable;

E. Whether Defendant owed a duty to Class members to safeguard their PII;

F. Whether Defendant breached a duty to Class members to safeguard their PII;

G. Whether computer hackers obtained Class members PII in the Data Breach;

H. Whether the Defendant knew or should have known that its data security systems and monitoring processes were deficient;

I. Whether the Plaintiff and Class members suffered legally cognizable injuries as a result of the Defendant's misconduct;

J. Whether Defendant's conduct was negligent;

K. Whether Defendant failed to provide notice of the Data Breach in a timely manner;

L. Whether Plaintiff and Class members are entitled to damages, civil penalties, and/or injunctive relief;

89. **Typicality.** Plaintiff's claims are typical of those of other Class members because Plaintiff's PII, like that of every other Class member, was compromised in the Data Breach.

90. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's Counsel are competent and experienced in litigating Class actions.

91. **Predominance.** Defendant has engaged in a common course of conduct toward Plaintiff and Class members, in that all of Plaintiff's and Class members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

92. **Superiority.** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

93. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

## VI. CAUSES OF ACTION

### COUNT I - Negligence
**(By Plaintiff on behalf of the Class, or, in the alternative, the Texas Subclass)**

94. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in preceding paragraphs.

95. As a condition of receiving their mortgages from partners of Defendant, Defendant's current and former customers were obligated to provide and entrust Defendant with certain PII, including their name, Social Security number, and information provided in connection with educational services.

96. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

97. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed or obtained by unauthorized parties.

98. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of its current and former customers' PII involved an unreasonable risk of harm to Plaintiff and the Class, including harm that foreseeably could occur through the criminal acts of a third party.

99. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiff's and Class members' information in Defendant's possession was adequately secured and protected.

100. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former customers' PII it was no longer required to retain pursuant to regulations.

101. Defendant had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff and Class members' PII, and to employ proper procedures to prevent the unauthorized dissemination of their PII.

102. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and Class members entrusted Defendant with their confidential PII, a mandatory step in obtaining services from Defendant.

103. Defendant were subject to an "independent duty," untethered to any contract between Defendant and Plaintiff and the Class, to maintain adequate data security.

104. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class members was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

105. Plaintiff and the members of the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing Plaintiff's and Class members' PII, the critical importance of adequately safeguarding that PII, and the necessity of encrypting PII stored on Defendant's systems.

106. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Class members. Defendant's wrongful conduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decision not to comply with industry standards for the safekeeping of Plaintiff's and Class members' PII, including basic encryption techniques available to Defendant.

107. Plaintiff and the Class had no ability to protect their PII that was in, and remains in, Defendant's possession.

108. Defendant was in a position to effectively protect against the harm suffered by Plaintiff and Class members as a result of the Data Breach.

109. Defendant had and continues to have a duty to adequately disclose that the PII belonging to Plaintiff and Class members that was in Defendant's possession was compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and Class members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

110. Defendant has admitted that Plaintiff's and Class members' PII was wrongfully accessed by unauthorized third persons as a result of the Data Breach.

111. Defendant, through its actions and inaction, unlawfully breached its duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding Plaintiff's and Class members' PII when the PII was within Defendant's possession or control.

112. Defendant improperly and inadequately safeguarded Plaintiff's and Class members' PII in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

113. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect its current and former customers' PII in the face of increased risk of theft.

114. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of their PII.

115. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove former customers' PII it was no longer required to retain pursuant to regulations.

116. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and Class members the existence and scope of the Data Breach.

117. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, Plaintiff's and Class members' PII would not have been compromised.

118. There is a close causal connection between (a) Defendant's failure to implement security measures to protect Plaintiff's and Class members' PII and (b) the harm or risk of imminent harm suffered by Plaintiff and the Class. Plaintiff's and Class members' PII was accessed and exfiltrated as the direct and proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

119. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of businesses, such as Defendant, of failing to implement reasonable measures to protect PII. The FTC Act and related authorities form part of the basis of Defendant's duty in this regard.

120. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the damages that would result to Plaintiff and Class members.

121. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

122. Plaintiff and Class members are within the class of persons that the FTC Act was intended to protect.

123. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

124. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and other identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the current and former customers' PII in its continued possession; and (viii) present and future costs in the form of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the compromise of PII as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class members.

125. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm,

including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

126. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

127. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and members of the Class are now at an increased risk of identity theft or fraud.

128. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class are entitled to and demand actual, consequential, and nominal damages and injunctive relief to be determined at trial.

**COUNT II – Breach of Implied Contract**
**(By Plaintiff on behalf of the Class, or, in the alternative, the Texas Subclass)**

129. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

130. This count is brought on behalf of all Class members.

131. Plaintiff and the Class provided Defendant with their PII.

132. By providing their PII, and upon Defendant's acceptance of such information, Plaintiff and Class members, on one hand, and Defendant, on the other hand, entered into implied-in-fact contracts for the provision of data security, separate and apart from any express contract entered into between the parties.

133. The implied contracts between Defendant and Plaintiff and Class members obligated Defendant to take reasonable steps to secure, protect, safeguard, and keep confidential Plaintiff's and Class members' PII. The terms of these implied contracts are described in federal

laws, state laws, and industry standards, as alleged above. Defendant expressly adopted and assented to these terms in its public statements, representations and promises as described above.

134. The implied contracts for data security also obligated Defendant to provide Plaintiff and Class members with prompt, timely, and sufficient notice of any and all unauthorized access or theft of their PII.

135. Defendant breached the implied contracts by failing to take, develop and implement adequate policies and procedures to safeguard, protect, and secure the PII belonging to Plaintiff and Class members; allowing unauthorized persons to access Plaintiff's and Class members' PII; and failing to provide prompt, timely, and sufficient notice of the Data Breach to Plaintiff and Class members, as alleged above.

136. As a direct and proximate result of Defendant's breaches of the implied contracts, Plaintiff and the Class have been damaged as described herein, will continue to suffer injuries as detailed above due to the continued risk of exposure of their PII in Defendant's possession, and are entitled to damages in an amount to be proven at trial.

**COUNT III – Breach of Confidence**
**(By Plaintiff on behalf of the Class, or, in the alternative, the Texas Subclass)**

137. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

138. At all times during Plaintiff's and Class members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff' and Class members' PII that Plaintiff and Class members provided to Defendant.

139. As alleged herein and above, Defendant's relationship with Plaintiff and Class members was governed by terms and expectations that Plaintiff's and Class members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

140. Plaintiff and Class members provided their respective PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the information to be disseminated to any unauthorized parties.

141. Plaintiff and Class members also provided their PII to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that PII from unauthorized disclosure, such as following basic principles of protecting its networks and data systems.

142. Defendant required and voluntarily received, in confidence, Plaintiff's and Class members' PII with the understanding that the information would not be disclosed or disseminated to the public or any unauthorized third parties.

143. Due to Defendant's failure to prevent, detect, and avoid the Data Breach from occurring by, *inter alia*, following best information security practices to secure Plaintiff's and Class members' PII, Plaintiff's and Class members' PII was disclosed to, and misappropriated by, unauthorized third parties beyond Plaintiff's and Class members' confidence, and without their express permission. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class members have suffered, and will continue to suffer damages.

144. But for Defendant's disclosure of Plaintiff's and Class members' PII in violation of the parties' understanding of confidence, Plaintiff's and Class members' PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class members' PII, as well as the resulting damages.

145. The injury and harm Plaintiff and Class members suffered, and continue to suffer, was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and

Class members' PII. Defendant knew its computer systems and technologies for accepting and securing Plaintiff's and Class members' PII had numerous security and other vulnerabilities placing Plaintiff's and Class members' PII in jeopardy.

146. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the compromise, publication, and/or theft of their PII; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession; (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class members; and (g) the diminished value of Defendant's services they received.

147. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non–economic losses.

**COUNT IV – Violation of State Data Breach Statutes**
**(By Plaintiff on behalf of the Class, or, in the alternative, the Texas Subclass)**

148. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

149. This count is brought on behalf of all Class members.

150. Defendant is a corporation that owns, maintains, and records PII, and computerized data including PII, about its customers' current and former customers, including Plaintiff and Class members.

151. Defendant is in possession of PII belonging to Plaintiff and Class members and is responsible for reasonably safeguarding that PII consistent with the requirements of the applicable laws pertaining hereto.

152. Defendant failed to safeguard, maintain, and dispose of, as required, the PII within its possession, custody, or control as discussed herein, which it was required to do by all applicable State laws.

153. Defendant, knowing and/or reasonably believing that Plaintiff's and Class members' PII was acquired by unauthorized persons during the Data Breach, failed to provide reasonable and timely notice of the Data Breach to Plaintiff and Class members as required by following data breach statutes.

154. Defendant's failure to provide timely and accurate notice of the Data Breach violated the following state data breach statutes:

a. Alaska Stat. Ann. § 45.48.010(a), *et seq.*;

b. Ark. Code Ann. § 4-110-105(a), *et seq.*;

c. Cal. Civ. Code § 1798.80, *et seq.*;

d. Colo. Rev. Stat. Ann § 6-1-716(2), *et seq.*;

e. Conn. Gen. Stat. Ann. § 36a-701b(b), *et seq.*;

f. Del. Code Ann. Tit. 6 § 12B-102(a), *et seq.*;

g. D.C. Code § 28-3852(a), *et seq.*;

h. Fla. Stat. Ann. § 501.171(4), *et seq.*;

i. Ga. Code Ann. § 10-1-912(a), *et seq.*;

j. Haw. Rev. Stat. § 487N-2(a), *et seq.*;

k. Idaho Code Ann. § 28-51-105(1), *et seq.*;

l. Ill. Comp. Stat. Ann. 530/10(a), *et seq.*;

m. Iowa Code Ann. § 715C.2(1), *et seq.*;

n. Kan. Stat. Ann. § 50-7a02(a), *et seq.*;

o. Ky. Rev. Stat. Ann. § 365.732(2), *et seq.*;

p. La. Rev. Stat. Ann. § 51:3074(A), *et seq.*;

q. Md. Code Ann., Commercial Law § 14-3504(b), *et seq.*;

r. Mass. Gen. Laws Ann. Ch. 93H § 3(a), *et seq.*;

s. Mich. Comp. Laws Ann. § 445.72(1), *et seq.*;

t. Minn. Stat. Ann. § 325E.61(1)(a), *et seq.*;

u. Mont. Code Ann. § 30-14-1704(1), *et seq.*;

v. Neb. Rev. Stat. Ann. § 87-803(1), *et seq.*;

w. Nev. Rev. Stat. Ann. § 603A.220(1), *et seq.*;

x. N.H. Rev. Stat. Ann. § 359-C:20(1)(a), *et seq.*;

y. N.J. Stat. Ann. § 56:8-163(a), *et seq.*;

z. N.C. Gen. Stat. Ann. § 75-65(a), *et seq.*;

aa. N.D. Cent. Code Ann. § 51-30-02, *et seq.*;

bb. Okla. Stat. Ann. Tit. 24 § 163(A), *et seq.*;

cc. Or. Rev. Stat. Ann. § 646A.604(1), *et seq.*;

dd. R.I. Gen. Laws Ann. § 11-49.3-4(a)(1), *et seq.*;

ee. S.C. Code Ann. § 39-1-90(A), *et seq.*;

ff. Tenn. Code Ann. § 47-18-2107(b), *et seq.*;

gg. Tex. Bus. & Com. Code Ann. § 521.053(b), *et seq.*;

hh. Utah Code Ann. § 13-44-202(1), *et seq.*;

ii. Va. Code. Ann. § 18.2-186.6(B), *et seq.*;

jj. Wash. Rev. Code Ann. § 19.255.010(1), *et seq.*;

kk. Wis. Stat. Ann. § 134.98(2), *et seq.*; and

ll. Wyo. Stat. Ann. § 40-12-502(a), *et seq.*

155. As a result of Defendant's failure to reasonably safeguard Plaintiff's and Class members' PII, and the failure to provide reasonable and timely notice of the Data Breach to Plaintiff and Class members, Plaintiff and the Class have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PII in Defendant's possession, and are entitled to damages in an amount to be proven at trial.

**COUNT V – Violation of State Consumer Protection Statutes**
**(By Plaintiff on behalf of the Class, or, in the alternative, the Texas Subclass)**

156. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

157. This count is brought on behalf of all Class members.

158. Defendant is a "person" as defined in the relevant state consumer statutes.

159. Defendant engaged in the conduct alleged herein that was intended to result, and which did result, in the trade and commerce with Plaintiff and Class members. Defendant is engaged in, and its acts and omissions affect, trade and commerce. Further, Defendant's conduct implicates consumer protection concerns generally.

160. Defendant's acts, practices and omissions were done in the course of Defendant's business of marketing, facilitating, offering for sale, and selling goods and services throughout the United States.

161. Defendant's unlawful, unfair, deceptive, fraudulent and/or unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the industry, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including but not limited to duties imposed by the FTC Act and similar state laws, rules, and regulations, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and the Class members' PII;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' PII;

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and Class members' PII; and

h. Failing to promptly and adequately notify Plaintiff and Class members that their PII was accessed by unauthorized persons in the Data Breach.

162. By engaging in such conduct and omissions of material facts, Defendant has violated state consumer laws prohibiting representing that "goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have," representing that "goods and services are of a particular standard, quality or grade, if they are of another", and/or "engaging in any other conduct which similarly creates a likelihood of confusion

or of misunderstanding"; and state consumer laws prohibiting unfair methods of competition and unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices.

163. Defendant's representations and omissions were material because they were likely to deceive reasonable persons about the adequacy of Defendant's data security and ability to protect the confidentiality of PII.

164. Defendant intentionally, knowingly, and maliciously misled Plaintiff and Class members and induced them to rely on its misrepresentations and omissions.

165. Had Defendant disclosed that its data systems were not secure and, thus, vulnerable to attack, it would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendant received, maintained, and compiled Plaintiff's and Class members' PII without advising that Defendant's data security practices were insufficient to maintain the safety and confidentiality of their PII. Accordingly, Plaintiff and the Class members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

166. Past breaches within the industry and against Defendant itself put Defendant on notice that its security and privacy protections were inadequate.

167. Defendant's practices were also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected in laws like the IDSCPA, CCPA, and the FTC Act.

168. The harm these practices caused to Plaintiff and the Class members outweighed their utility, if any.

169. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiff and Class members as a direct result of Defendant's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and/or unlawful acts or practices as set forth herein include, without limitation:

a. unauthorized charges on their debit and credit card accounts;

b. theft of their PII;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse effects on their credit scores and adverse credit notations;

e. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate and mitigate the actual and future consequences of the Data Breach, including without limitation finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

f. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. damages to and diminution in value of their personal and financial information entrusted to Defendant and with the understanding that Defendant would safeguard their data against theft and not allow access and misuse of their data by others; and

h. the continued risk to their PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect data in its possession.

170. Defendant's conduct described herein, including without limitation, Defendant's failure to maintain adequate computer systems and data security practices to safeguard Plaintiff's and Class members' PII, Defendant's failure to disclose the material fact that it did not have

adequate computer systems and safeguards to adequately protect Plaintiff's and Class members' PII, Defendant's failure to provide timely and accurate notice to of the material fact of the Data Breach, and Defendant's continued acceptance of Plaintiff's and Class members' PII constitute unfair methods of competition and unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices in violation of the following state consumer statutes:

a. The Alabama Deceptive Trade Practices Act, Ala. Code § 8-19-5(5), (7) and (27), *et seq*.;

b. The Arizona Consumer Fraud Act, A.R.S. § 44-1522;

c. The Arkansas Deceptive Trade Practices Act, Ark. Code Ann. §§ 4-88-107(a)(1)(10) and 4-88-108(1)(2), *et seq*.;

d. The California Consumer Legal Remedies Act, Cal. Civ. Code § 1750, *et seq*., and the California Unfair Competition Law, Cal. Bus. and Prof. Code, § 17200, *et seq.*;

e. The Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. § 42-110(b), *et seq*.;

f. The Delaware Deceptive Trade Practices Act, Del. Code Ann. Title 6, § 2532(5) and (7), *et seq*., and the Delaware Consumer Fraud Act, Del. Code Ann. Title 6 § 2513, *et seq*.;

g. The Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. Ann. § 501.204(1), *et seq*.;

h. The Georgia Fair Business Practices Act, Ga. Code Ann. §§ 10-1-393(a) and (b)(2), (5) and (7), *et seq.*;

i. The Hawaii Deceptive Trade Practices Act, Haw. Rev. Stat. Ann. §§ 481A-3(a)(5), (7) and (12), *et seq.*; and the Hawaii Consumer Protection Act, Haw. Rev. Stat. Ann. § 480-2(a), *et seq.*;

j. The Idaho Consumer Protection Act, Idaho Code §§ 48-603(5), (7), (17) and (18), *et seq.*; and Idaho Code § 48-603C, *et seq.*;

k. The Illinois Consumer Fraud and Deceptive Trade Practices Act, 815 Ill. Stat. § 505/2, *et seq.*;

l. The Indiana Deceptive Consumer Sales Act, Ind. Code §§ 24-5-0.5-3(a) and (b)(1) and (2), *et seq.*;

m. The Iowa Consumer Fraud Act, I.C.A. §§ 714H.3 and 714H.5, *et seq.*;

n. The Kansas Consumer Protection Act, Kan. Stat. §§ 50-626(a) and (b)(1)(A)(D) and (b)(3), *et seq.*;

o. The Kentucky Consumer Protection Act, K.R.S. § 367.170(1) and (2), *et seq.*;

p. The Louisiana Unfair Trade Practices and Consumer Protection Law, La. Rev. Stat. Ann. § 51:1405(A), *et seq.*;

q. The Maine Uniform Deceptive Trade Practices Act, 10 M.R.S.A. §§ 1212(1)(E) and (G), e*t seq.*, and the Maine Unfair Trade Practices Act, 5 M.R.S.A. § 207, *et seq.*;

r. The Maryland Consumer Protection Act, Md. Code Commercial Law, § 13-301(1) and (2)(i), and (iv) and (9)(i), *et seq.*;

s. The Massachusetts Consumer Protection Act, Ma. Gen. Laws Ann. Ch. 93A § 2(a), *et seq.*;

t. The Michigan Consumer Protection Act, M.C.P.L.A. § 445.903(1)(c)(e),(s) and (cc), *et seq.*;

u. The Minnesota Uniform Deceptive Trade Practices Act, Minn. Stat. § 325D.44, subd. 1(5), (7) and (13), et seq., the Minnesota Consumer Fraud Act, Minn. Stat. § 325F.69, subd. 1, and Minn. Stat. § 8.31, subd. 3(a);

v. The Mississippi Consumer Protection Act, Miss. Code Ann. §§ 75-24-5(1), (2)(e) and (g), *et seq.*;

w. The Missouri Merchandising Practices Act, Mo. Ann. Stat. § 407.020(1), *et seq.*;

x. The Montana Unfair Trade Practices and Consumer Protection Act, MCA §§ 30-14-103, *et seq.*;

y. The Nebraska Consumer Protection Act, Neb. Rev. Stat. § 59-1602, and the Nebraska Uniform Deceptive Trade Practices Act, Neb. Rev. Stat. § 87-302(a)(5) and (7), *et seq.*;

z. The Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. Ann. § 598.0915(5) and (7), *et seq.*;

aa. The New Hampshire Consumer Protection Act, N.H. Rev. Stat. Ann. § 358-A:2(v) and (vii), *et seq.*;

bb. The New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8-2, *et seq.*;

cc. The New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-2(D)(5)(7) and (14) and 57-12-3, *et seq*.;

dd. New York Business Law, N.Y. Gen. Bus. Law § 349(a);

ee. The North Carolina Unfair Trade Practices Act N.C.G.S.A. § 75-1.1(a), *et seq*.;

ff. The North Dakota Unlawful Sales or Advertising Practices Act, N.D. Cent. Code § 51-15-02, *et seq*.;

gg. The Ohio Consumer Sales Practices Act, Ohio Rev. Code Ann. § 1345.02(A) and (B)(1) and (2), *et seq.*;

hh. The Oklahoma Consumer Protection Act, 15 Okl. Stat. Ann. § 753(5), (7) and (20), *et seq.*; and the Oklahoma Deceptive Trade Practices Act, 78 Okl. Stat. Ann. § 53(A)(5) and (7), *et seq.*;

ii. The Oregon Unfair Trade Practices Act, Or. Rev. Stat. § 646.608(1)(e)(g) and (u), *et seq.*;

jj. The Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-2(4)(v)(vii) and (xxi), and 201-3, *et seq*.;

kk. The Rhode Island Deceptive Trade Practices Act, R.I. Gen. Laws § 6-13.1-1(6)(v), (vii), (xii), (xiii) and (xiv), *et seq.*;

ll. The South Carolina Unfair Trade Practices Act, S.C. Code Ann. § 39-5-20(a), *et seq.*;

mm. The South Dakota Deceptive Trade Practices Act and Consumer Protection Act, S.D. Codified Laws § 37-24-6(1), *et seq*.;

nn. The Tennessee Consumer Protection Act, Tenn. Code Ann. §§ 47-18-104(a) and (b)(5) and (7);

oo. The Texas Deceptive Trade Practices- Consumer Protection Act, V.T.C.A., Bus. & C. § 17.46(a), (b)(5) and (7), *et seq*.;

pp. The Utah Consumer Sales Practices Act, Utah Code Ann. §§ 13-11-4(1) and (2)(a) and (b);

qq. The Vermont Consumer Fraud Act, 9 V.S.A. § 2453(a), *et seq.*;

rr. The Virginia Consumer Protection Act, Va. Code Ann. § 59.1-200(A)(5)(6) and (14), *et seq.*;

ss. The Washington Consumer Protection Act, Wash. Rev. Code § 19.86.020, *et seq*.;

tt. The West Virginia Consumer Credit and Protection Act, W.V.A. Code § 46A-6-104, *et seq*.;

uu. The Wisconsin Deceptive Trade Practices Act, W.S.A. § 100.20(1), *et seq.*; and

vv. The Wyoming Consumer Protection Act, Wyo. Stat. Ann. § 40-12-105(a), (i), (iii) and (xv), *et seq*.

171. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring Defendant from disclosing their PII without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

## VII. PRAYER FOR RELIEF

172. WHEREFORE, Plaintiff, on behalf of herself and all Class members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class as defined herein, and appointing Plaintiff and their counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and the Class members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personally identifying information of Plaintiff and Class members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personally identifying information of Plaintiff and Class members;

v. prohibiting Defendant from maintaining Plaintiff's and Class members' PII on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other areas of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personally identifying information, as well as protecting the personally identifying information of Plaintiff and Class members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personally identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to adequately educate all Class members about the threats that they face as a result of the loss of their confidential personally identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and, for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to Class Counsel, and to report any material deficiencies or noncompliance with the Court's final judgment;

D. For an award of damages, including actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of reasonable attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

## VIII. JURY TRIAL DEMAND

173. Plaintiff hereby demands that this matter be tried before a jury.

DATED: April 13, 2022

Respectfully submitted,

*/s/Joe Kendall*
JOE KENDALL
Texas Bar No. 11260700
**KENDALL LAW GROUP, PLLC**
3811 Turtle Creek Blvd., Suite 1450
Dallas, Texas 75219
214-744-3000 / 214-744-3015 (Facsimile)
jkendall@kendalllawgroup.com

Gary M. Klinger*
**MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC**
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
Email: **gklinger@milberg.com**

David K. Lietz*
**MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC**
5335 Wisconsin Avenue NW
Suite 440
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877
Email: **dlietz@milberg.com**

Daniel O. Herrera*
Nickolas J. Hagman*
**CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP**
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
dherrera@caffertyclobes.com
nhagman@caffertyclobes.com

***Attorneys for Plaintiff and the Proposed Class***

**pro hac vice forthcoming*